What Is Claimed Is:

1. A method for managing encryption within a database system that is managed by a security administrator, wherein encryption is performed automatically and transparently to a user of the database system, wherein users of the database system are managed by a user administrator, the method comprising:

receiving a request to store data in a column of the database system, wherein the column is designated as an encrypted column;

in response to receiving the request, automatically encrypting data using an encryption function, wherein the encryption function uses a key stored in a keyfile managed by the security administrator; and

storing data in the database system using a storage function of the database system.

2. The method of claim 1, further comprising:

receiving a request to retrieve data from the encrypted column of the database system;

if the request to retrieve data is received from the database administrator, preventing the database administrator from decrypting encrypted data;

if the request to retrieve data is received from the security administrator, preventing the security administrator from decrypting encrypted data; and

if the request to retrieve data is from an authorized user of the database system, allowing the authorized user to decrypt encrypted data.

3. The method of claim 1, wherein the security administrator selects one of, data encryption standard (DES) and triple DES as a mode of encryption for the column.

4. The method of claim 1, wherein the security administrator, the database administrator, and the user administrator are distinct roles, and wherein a person selected for one of these roles is not allowed to be selected for another of these roles.

5. The method of claim 1, wherein managing the keyfile includes, but is not limited to:

creating the keyfile;

establishing a plurality of keys to be stored in the keyfile;

establishing a relationship between a key identifier and the key stored in the keyfile;

storing the keyfile in one of,

an encrypted file in the database system, and

a location separate from the database system; and

moving an obfuscated copy of the keyfile to a volatile memory within a server associated with the database system.

6. The method of claim 1, wherein upon receiving a request from the security administrator specifying the column to be encrypted, if the column currently contains data, the method further comprises:

decrypting the column using an old key if the column was previously encrypted; and

encrypting the column using a new key.

7. The method of claim 5, wherein the key identifier associated with the encrypted column is stored as metadata associated with a table containing the encrypted column within the database system.

8. The method of claim 5, further comprising establishing encryption parameters for the encrypted column, wherein the encryption parameters include encryption mode, key length, and integrity type by:

entering encryption parameters for the encrypted column manually; and

recovering encryption parameters for the encrypted column from a profile table in the database system.

9. A computer-readable storage medium storing instructions that when executed by a computer causes the computer to perform a method for managing encryption within a database system that is managed by a security administrator, wherein encryption is performed automatically and transparently to a user of the database system, wherein users of the database system are managed by a user administrator, the method comprising:

receiving a request to store data in a column of the database system, wherein the column is designated as an encrypted column;

in response to receiving the request, automatically encrypting data using an encryption function, wherein the encryption function uses a key stored in a keyfile managed by the security administrator; and

storing data in the database system using a storage function of the database system.

10. The computer-readable storage medium of claim 9, the method further comprises:

receiving a request to retrieve data from the encrypted column of the database system;

if the request to retrieve data is received from the database administrator, preventing the database administrator from decrypting encrypted data;

if the request to retrieve data is received from the security administrator, preventing the security administrator from decrypting encrypted data; and

if the request to retrieve data is from an authorized user of the database system, allowing the authorized user to decrypt encrypted data.

11. The computer-readable storage medium of claim 9, wherein the security administrator selects one of, data encryption standard (DES) and triple DES as a mode of encryption for the column.

12. The computer-readable storage medium of claim 9, wherein the security administrator, the database administrator, and the user administrator are distinct roles, and wherein a person selected for one of these roles is not allowed to be selected for another of these roles.

13. The computer-readable storage medium of claim 9, wherein managing the keyfile includes, but is not limited to:

creating the keyfile;

establishing a plurality of keys to be stored in the keyfile;

establishing a relationship between a key identifier and the key stored in the keyfile;

storing the keyfile in one of,

an encrypted file in the database system, and

a location separate from the database system; and moving an obfuscated copy of the keyfile to a volatile memory within a server associated with the database system.

14. The computer-readable storage medium of claim 9, wherein upon receiving a request from the security administrator specifying the column to be encrypted, if the column currently contains data, the method further comprises:

decrypting the column using an old key if the column was previously encrypted; and

encrypting the column using a new key.

15. The computer-readable storage medium of claim 13, wherein the key identifier associated with the encrypted column is stored as metadata associated with a table containing the encrypted column within the database system.

16. The computer-readable storage medium of claim 13, wherein the method further comprises establishing encryption parameters for the encrypted column, wherein the encryption parameters include encryption mode, key length, and integrity type by:

entering encryption parameters for the encrypted column manually; and

recovering encryption parameters for the encrypted column from a profile table in the database system.

17. An apparatus that facilitates managing encryption within a database system that is managed by a security administrator, wherein encryption is performed automatically and transparently to a user of the database system,

wherein users of the database system are managed by a user administrator, comprising:

a receiving mechanism that is configured to receive a request to store data in a column of the database system, wherein the column is designated as an encrypted column;

an encrypting mechanism that is configured to encrypt data using an encryption function, wherein the encryption function uses a key stored in a keyfile managed by the security administrator; and

a storing mechanism that is configured to store data in the database system using a storage function of the database system.

18. The apparatus of claim 17, further comprising:

the receiving mechanism that is further configured to receive a request to retrieve data from the encrypted column of the database system;

an access mechanism that is configured to prevent the database administrator and the security administrator from decrypting encrypted data; and

wherein the access mechanism is configured to allow an authorized user of the database system to decrypt encrypted data.

19. The apparatus of claim 17, further comprising a selection mechanism that is configured to select one of, data encryption standard (DES) and triple DES as a mode of encryption for the column.

20. The apparatus of claim 17, wherein the security administrator, the database administrator, and the user administrator are distinct roles, and wherein a person selected for one of these roles is not allowed to be selected for another of these roles.

21. The apparatus of claim 17, further comprising:

a creating mechanism that is configured to create the keyfile;

an establishing mechanism that is configured to establish a plurality of keys to be stored in the keyfile;

wherein the establishing mechanism is further configured to establish a relationship between a key identifier and the key stored in the keyfile;

a storing mechanism that is configured to store the keyfile in one of,

an encrypted file in the database system, and

a location separate from the database system; and

a moving mechanism that is configured to move an obfuscated copy of the keyfile to a volatile memory within a server associated with the database system.

22. The apparatus of claim 17, further comprising:

a decrypting mechanism that is configured to decrypt the column using a previous key if the column was previously encrypted; and

wherein the encrypting mechanism is further configured to encrypt the column using a new key.

23. The apparatus of claim 21, wherein the key identifier associated with the encrypted column is stored as metadata associated with a table containing the encrypted column within the database system.

24. The apparatus of claim 21, wherein the establishing mechanism is further configured to establish encryption parameters for the encrypted column, wherein encryption parameters include encryption mode, key length, and integrity type, and wherein the establishing mechanism includes:

an entering mechanism that is configured to enter encryption parameters for the encrypted column manually; and

a recovering mechanism that is configured to recover encryption parameters for the encrypted column from a profile table in the database system.

Add a1